[19]中华人民共和国国家知识产权局

[51]Int.Cl⁷
H04L 12/40
H04L 9/00

# [12]发明专利申请公开说明书

[21]申请号 98804411.0

[43]公开日 2000年5月10日

[11]公开号 CN 1252912A

[22]申请日 1998.4.22 [21]申请号 98804411.0
[30]优先权
[32]1997.4.24 [33]JP [31]106995/1997
[86]国际申请 PCT/JP98/01837 1998.4.22
[87]国际公布 WO98/48543 日 1998.10.29
[85]进入国家阶段日期 1999.10.22
[71]申请人 松下电器产业株式会社
地址 日本大阪府
[72]发明人 西村拓也 饭塚裕之
山田正纯

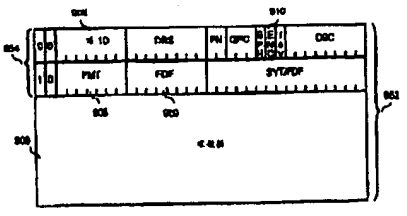
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马莹

权利要求书3页 说明书15页 附图页数7页

[54]发明名称 数据传送方法

[57]摘要

一种数据传送方法，其目的在于，在IEEE1394总线上对用著作权保护的AV信息进行加密来发送时，即使是不能应付加密的以往的设备也不会误操作，在用同步通信传送的同步数据中包含表示实数据部加密状况的加密识别信息和实数据部，加密只对实数据部进行。表示同步数据内实数据部加密状况的加密识别信息和实数据一起从发送装置发送，通过该加密识别信息检测出实数据部被加密的接收装置向发送装置请求解密信息，接收到根据该请求从发送装置发送的解密信息的接收装置使用该解密信息进行实数据部的解密。



ISSN1008-4274

# 权 利 要 求 书

1、一种数据传送方法，用于使用同步(isochronous)通信和异步(asynchronous)通信的总线系统，在该同步通信中总线上的任意设备接收同步数据，而在该异步通信中接收异步数据的设备被指定，其特征在于，上述同步数据有时包含实数据部，表示上述实数据部加密状况的加密识别信息包含在上述实数据部以外的上述同步数据中，接收到上述同步数据的接收装置在上述加密识别信息指示上述实数据部被加密的情况下，向发送上述同步数据的发送装置使用上述异步通信请求上述实数据部的解密信息，接收到上述请求的上述发送装置使用上述异步通信向上述接收装置发送对上述实数据部的上述解密信息进行加密的加密信息、或者取得上述解密信息所需的解密信息取得数据，上述接收装置在接收到上述加密过的解密信息的情况下，从上述加密过的解密信息中取出上述解密信息，而在上述接收装置接收到上述解密信息取得数据的情况下，使用上述解密信息取得数据来取得上述解密信息，使用这样得到的上述解密信息对加密过的实数据部进行解密。

2、如权利要求 1 所述的数据传送方法，其特征在于，接收到上述同步数据的上述接收装置检测出上述实数据部被加密之后、直至取得上述解密信息的一系列过程有多种，所述接收装置在请求上述解密信息之前，先向上述发送装置询问上述发送装置能够执行的过程的种类，上述接收装置从自身和上述发送装置双方都能够执行的过程中选择执行的过程，上述接收装置根据选择出的上述过程来取得上述解密信息。

3、如权利要求 2 所述的数据传送方法，其特征在于，在上述发送装置和上述接收装置双方都能够执行的上述过程存在多个的情况下，根据预定的优先级来选择上述过程。

4、如权利要求 1 所述的数据传送方法，其特征在于，接收到上述同步数据的上述接收装置检测出上述实数据部被加密之后、直至取得上述解密信息的上述一系列过程有多种，上述接收装置从上述多种过程中根据预定的优先级来选择上述过程并开始上述过程，在上述发送装置不能执行上述接收装置选择出的上述过程的情况下，上述接收装置依次重新选择上述过程，直至找到上述发送装置能够执行的上述过程并开始上述过程，上述接收装置在找到能够执行的过程时，根据该选择出的过程来取得上述解密信息。

5、如权利要求 2~4 中任一项所述的数据传送方法，其特征在于，根据上述选择出的过程，在上述发送装置和上述接收装置之间授受的上述异步数据中，包含表示执行中的上述过程的种类的标识符。

6、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，上述接收装置在进行上述解密信息的请求之前，确认上述发送装置是正规的发送装置。

7、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，上述发送装置在接收到上述解密信息的请求后，在接收装置确认是上述正规的接收装置之后，对上述实数据部的解密信息进行加密并发送。

8、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，上述发送装置和上述接收装置在相互确认对方是上述正规的接收装置或上述正规的发送装置之后，上述接收装置进行上述解密信息的请求。

9、如权利要求 1~8 中任一项所述的数据传送方法，其特征在于，在上述接收装置请求上述解密信息之前，从上述接收装置向上述发送装置发送上述发送装置制作公共密钥至少必须的信息，并且从上述发送装置向上述接收装置发送上述接收装置制作上述公共密钥至少必须的信息，上述发送装置使用上述公共密钥对上述解密信息进行加密并发送，上述接收装置从接收到的上述加密过的复合化信息中使用上述公共密钥来取出上述解密信息。

10、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，上述加密只对上述实数据部进行。

11、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，上述发送装置内部具有实数据的信号源，上述发送装置对从上述信号源输出的以固定长度为单位的每个上述实数据决定加密的有无，将加密过的上述实数据和未加密的上述实数据配置在相互不同的上述同步通信的输出单位内，输出到上述总线系统。

12、如权利要求 11 所述的数据传送方法，其特征在于，上述接收装置使用上述异步通信向上述发送装置指定上述加密过的实数据和上述未加密的实数据的比率，上述发送装置根据上述指定来变更加密有无的比率。

13、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，上述发送装置内部具有上述实数据的信号源，上述发送装置对从上述信号源输出的上述以固定长度为单位的实数据，决定上述以固定长度为单位的实数据中

进行上述加密的比例，将上述实数据配置到上述同步通信的输出单位内，输出到上述总线系统。

14、如权利要求 13 所述的数据传送方法，其特征在于，上述接收装置通过上述异步通信向上述发送装置指定进行上述加密的比例，上述发送装置根据上述指定来变更上述加密的比例。

15、如权利要求 1~5 中任一项所述的数据传送方法，其特征在于，在上述发送装置发送上述同步数据时，至少在请求上述解密信息之前的期间内在上述同步数据中不包含上述实数据部来发送，至少在接收到上述解密信息后开始发送包含上述实数据部的上述同步数据。

# 说 明 书

## 数据传送方法

技术领域

本发明涉及一种数字数据传送方法，用于传送通常的数字数据和加密过的数字数据混合而成的数据。

背景技术

在以往的数据传送方式中，有使用 IEEE1394 标准(IEEE: THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.，美国电气与电子工程师学会)的数据传送方法(参考文献：IEEE Std 1394: 1995, High Performance Serial Bus(高性能串行总线))。在 IEEE1394 标准的数据传送中有：同步(isochronous)通信，适合传送数字图像信号和数字语音信号等同步数据；和异步(asynchronous)通信，适合传送控制信号等非同步数据。两者的通信都可以在 IEEE1394 总线上使用。同步通信是所谓的广播型的通信，IEEE1394 总线上的 1 个装置输出的同步分组，可以由该总线上的所有装置接收。与此相对，在异步通信中，有一对一的通信和一对 N 的广播型通信两种，在总线上的 1 个装置输出的异步分组中，包含表示要接收该分组的装置的标识符，在该标识符表示特定的装置时，由该标识符指定的装置接收该异步分组，而在该标识符表示广播时，由该总线上的所有装置接收该异步分组。

此外，作为使用 IEEE1394 标准的数据传送方法、传送数字语音信号和数字图像信号、或者在连接到 IEEE1394 总线上的设备间进行数据传送的标准，IEC(IEC: International Electrotechnical Commission，国际电工技术委员会)正在研究 IEC1883 标准(以下称为 AV 协议)。在 AV 协议中，图像语音数据被配置在图 5 所示的同步分组内进行传送。此外，同步分组包含 CIP 首标(CIP: Common Isochronous Packet，通用同步分组)。在 CIP 首标内，包含表示图像语音数据种类的标识信息、和发送同步分组的发送装置的装置号码等信息。

图 5 是 AV 协议中使用的同步分组的格式图。同步分组由同步分组首标

900、首标 CRC 901、同步净荷(payload)902 及数据 CRC 903 构成。在同步分组首标 900 中包含标记(tag)907。标记 907 的值为 1 时，表示该同步分组符合 AV 协议。当标记 907 的值为 1 时，即该同步分组是符合 AV 协议的分组时，在同步净荷 902 的头部包含 CIP 首标 904。在 CIP 首标 904 中，包含源 ID 906，它是输出该同步分组的输出装置的标识符。而在 CIP 首标 904 中包含 FMT 908 和 FDF 909，表示同步净荷 902 中包含的实数据 905 是什么样的数据。图像信号和语音信号的数字数据包含在实数据 905 中，而实数据 905 不一定要包含在同步净荷 902 中，因分组而异，可以有不包含实数据 905、而只包含 CIP 首标 904 的同步净荷 902。

此外，作为 AV 协议中用于进行设备控制的命令群，有 AV/C 命令集。(参考文献：1394 TRADE ASSOCIATION Specification for AV/C Digital Interface Command Set Version 1.0 September 13, 1996)这些命令及其响应使用异步通信来传送。

在上述以往的数据传送方法中，如果为了著作权保护而要以异步通信来发送将同步净荷 902 加密而得的同步分组，则不能保持与不能传送加密过的同步净荷 902 的以往的设备的兼容。即，以往的设备是以同步净荷 902 的头部正常配置有 CIP 首标 904 进行发送为前提而制造的，如果同步净荷 902 被加密，则用以往的设备不能正常读出 CIP 首标 904，而判断该同步分组不满足 AV 协议，从而接收加密过的同步分组的接收装置不能正常操作。即，用该接收装置不能判别实数据 905 中包含的数据是哪种数据，不能鉴别输出该同步分组的装置，而且不能对该发送装置进行各种询问等异步通信，所以不能正常进行接收操作。

此外，在上述以往的数据传送方法中，在接收装置连续接收发送装置输出的同步分组期间同步分组的加密开始的情况下，在以往的设备中，加密一开始，则不能正常读出 CIP 首标 904，不能进行正常的接收。

此外，为了使发送装置对用著作权保护的图像语音信息等进行加密来发送，而使被认为是正规的接收装置对该加密过的图像语音数据等进行解密，则发送装置必须向正规的接收装置提供解密所需的解密信息。在此情况下，在上述以往的数据传送方法中，发送装置要鉴别接收装置，必须执行非常烦杂的过程。即，在同步分组中包含源 ID 906，它是进行发送的装置的标识符，而不包含表示哪个装置应接收该同步分组的信息，因此，发送装置在同步分

组发送中不能检查哪个装置接收该同步分组。因此，为了使发送装置检查连接到 IEEE1394 总线上的设备中哪个设备正在进行接收，则发送装置必须对总线上的所有设备依次进行接收状态的询问，而提供解密所需的密钥信息的过程非常烦杂。

本发明就是为了解决上述以往的问题，其目的在于，实现一种数据传送方法，它在以同步通信发送加密过的图像语音信息的情况下也满足以往的通信标准，而且以往的接收装置接收包含加密过的图像语音数据的同步分组也不会误操作。

此外，本发明就是为了解决上述以往的问题，其目的在于，实现一种数据传送方法，它可以大大简化发送装置向正规的接收装置提供解密所需的密钥信息的过程。

发明概述

为了解决上述以往数据传送方法的问题，在本发明的数据传送方法中，在用同步通信传送的同步数据中包含表示实数据部加密状况的加密识别信息和实数据部，加密只对实数据部进行。

此外，为了解决上述以往数据传送方法的问题，在本发明的数据传送方法中，表示同步数据内实数据部加密状况的加密识别信息与实数据一起从发送装置发送，通过该加密识别信息检测出实数据部被加密的接收装置向发送装置请求解密信息，接收到根据该请求从发送装置发送的解密信息的接收装置使用该解密信息进行实数据部的解密，来进行数据传送。

在本发明的数据传送方法中，接收到同步数据的接收装置检查同步数据内包含的加密识别信息，如果检测出实数据部被加密，则向发送装置请求用于对实数据部进行解密的解密信息。该请求通过 AV/C 集中的命令使用异步通信来进行，在接收到该请求的发送装置中，通过检查接收到的命令的分组首标，来鉴别发出请求的设备、即接收装置。发送装置通过异步通信用命令向这里鉴别出的接收装置赋予解密信息，从而能够实现发送装置向接收装置赋予用于解密的解密信息的过程极其简单的数据传送方法。

此外，在本发明中，同步数据的加密只对实数据部进行，在同步数据中包含表示实数据部加密状况的加密识别信息。由此，CIP 首标不被加密而被原封不动地传送，所以即使以往的装置接收到这些加密过的同步数据也不会

误操作。即，能够实现一种数据传送方法，使得保持与以往数据传送方法的兼容性，而且即使以往的接收装置接收到加密过的同步数据也不可能误操作。

此外，在本发明的数据传送中，即使在接收装置连续接收发送装置发送的同步数据期间，同步数据的加密开始，CIP 首标也不被加密而被原封不动地传送，所以能够实现进行接收的接收装置不可能误操作的数据传送方法。

附图的简单说明

图 1 是本发明实施例中 CIP 首标的格式示意图；

图 2 是本发明实施例中发送装置和接收装置的功能方框图；

图 3A 是本发明实施例中 AKE 状态命令的格式图；

图 3B 是本发明实施例中与 AKE 状态命令对应的 AKE 响应的格式图；

图 3C 是本发明实施例中 AKE 控制命令的格式图；

图 4 是本发明实施例中在发送装置和接收装置之间传输的异步分组的传输过程示意图；

图 5 是以往的数据传送方法中同步分组的格式图。

实施发明的最好方式

下面，参照附图来说明本发明第一实施例。

图 1 是本发明实施例中传送的同步分组的净荷部的形式图。本实施例是符合 MPEG(Moving Picture Expert Group，运动图像专家组)的 TSP(transport packet，运输分组)的传送例。ENC(以下记作解密信息)910 表示实数据 905 是否被解密。

图 2 是本发明实施例中发送装置和接收装置的关系图。发送装置 110 和接收装置 128 通过 IEEE1394 总线(以下记作 1394 总线)111 连接。

下面首先说明发送装置 110 中各块的功能。

信号源 100 将要发送到 1394 总线 111 上的以 188 字节为单位的 MPEG 运输分组 TSP(未图示)输出到加密部件 101。即，在本实施例中，信号源 100 输出 188 字节的固定长度的数据。加密部件 101 使用密钥生成部件 106 提供的加密密钥 109 对从信号源 100 接收到的 TSP 进行加密并输出。在本实施例中，加密密钥 109 相当于解密信息。输出命令 105 是密钥生成部件 106 对

加密部件 101 的命令，有通常输出、加密输出及空输出 3 种命令。接收到输出命令 105 的加密部件 101 在该命令的内容是通常输出的情况下，原封不动地输出从信号源 100 接收到的 TSP，作为加密信息 910 而输出值 0。而在输出命令 105 的内容是加密输出的情况下，用从密钥生成部件 106 接收到的加密密钥 109 对 TSP 进行加密并输出，作为加密信息 910 而输出值 1。而在输出命令 105 的内容是空输出的情况下，每当从信号源 100 接收到 TSP 时就输出空信号(未图示)，同时作为加密信息 910 而输出值 1。源分组化部件 102 向从加密部件 101 接收到的 188 字节的 TSP 附加 4 字节的源分组首标，输出 192 字节的源分组(实数据 905)。CIP 块化部件 103 向从源分组部件 102 接收到的源分组附加 CIP 首标 954，输出同步净荷 952。此时，CIP 块化部件 103 将从加密部件 101 接收到的加密信息 910 配置到 CIP 首标 954 内。同步分组化部件 107 向从 CIP 块化部件 103 接收到的同步净荷 952 附加同步分组首标 900、首标 CRC 901 及数据 CRC 903，输出同步分组。此时，同步净荷 952 的内容是符合 AV 协议的数据，所以标记 907 的值为 1。密钥生成部件 106 如后所述在其与接收装置 128 之间，通过图 3 所示的异步分组的发收而将加密密钥 109 发送到接收装置 128；此外，如前所述，对加密部件 101 也输出加密密钥 109。

1394 分组输入输出部件 108 在 1394 总线 111 和接收装置 110 之间进行同步分组及异步分组的输入输出。即，1394 分组输入输出部件 108 将从同步分组化部件 107 接收到的同步分组、及从密钥生成部件 106 接收到的异步分组输出到 1394 总线 111 上，同时将从 1394 总线 111 接收到的异步分组输出到密钥生成部件 106。

下面接着说明接收装置 128 的各块的功能。

1394 分组输入输出部件 127 在 1394 总线 111 和接收装置 128 之间进行同步分组及异步分组的输入输出。即，1394 分组输入输出部件 127 将从 1394 总线 111 接收到的同步分组输出到净荷提取部件 123，将从 1394 总线接收到的异步分组输出到密钥生成部件 125。此外，将从密钥生成部件 125 接收到的异步分组输出到 1394 总线 111。

净荷提取部件 123 从 1394 分组输入输出部件 127 接收从 1394 总线 111 接收到的同步分组，在同步分组的标记 907 的值为 1 的情况下，知道同步净荷 952 的内容是符合 AV 协议的数据，将同步净荷 952 输出到实数据提取部

件 122。实数据提取部件 122 在接收到的同步净荷 952 中包含实数据 905 的情况下，将除去同步净荷 952 的头部的 CIP 首标 954 的实数据 905 输出到解密部件 121。此外，实数据提取部件 122 将从 CIP 首标 954 中提取出的源 ID 906 和加密信息 910 输出到密钥生成部件 125。此外，加密信息 910 也被输出到解密部件 121。密钥生成部件 125 如后所述在其与发送装置 110 之间通过由异步通信进行的异步分组的发收来接收加密密钥 126，将加密密钥输出到解密部件 121。解密部件 121 在从实数据提取部件 122 接收到的加密信息 910 的值为 0 时，将从实数据提取部件 122 接收到的实数据 905 原封不动地输出到图像语音化部件 120，而在加密信息 910 的值为 1 时，使用从密钥生成部件 125 接收到的加密密钥 126 对实数据 905 进行解密，将解密结果输出到图像语音化部件 120。

下面说明前述的由异步通信进行的异步分组传输。

图 3A~C 示出通过异步通信传输的异步分组的格式，其中图 3A 及图 3C 是本实施例中密钥生成部件 106 和密钥生成部件 125 之间发收的 AKE 命令(AKE: Authentication and Key Exchange，鉴证和密钥交换)的命令格式，而图 3B 是响应格式。这些命令及响应属于 AV/C 命令集，使用异步通信在发送装置 110 和接收装置 128 之间被发收。通过发收这些命令及响应，在发送装置 110 及接收装置 128 之间交换对方装置的认证和加密密钥 109、126 的发收所需的信息。在上述 AKE 命令中有：AKE 控制命令，用于请求对方装置进行某些操作；和 AKE 状态命令，用于询问对方装置的状态和能力。

图 3A 是 AKE 状态命令的格式图。在 AKE 状态命令中，操作码 208 表示该命令是 AKE 命令。算法 ID 200 是固定值 0，0 以外的值是为将来的扩展而保留的。

图 3B 表示对 AKE 状态命令的响应的格式。接收到图 3A 的 AKE 状态命令的装置对发布该 AKE 状态命令的装置返送的就是此响应。在发送装置 110 和接收装置 128 之间进行相互认证及加密密钥 109、126 的传达的一系列信息交换过程有多种，在算法区域 201 中比特指定(bit assign)有返回该响应的装置能够执行的信息交换过程的标识符。即，接收装置 128 在检测出通过上述过程加密的 TSP 之后、直至接收到加密密钥 109、126 这一期间内，在其与发送装置 110 之间发收多个命令及响应。发收该命令及响应的信息交换过程有多种，返回该响应的装置将算法区域 201 中对应的比特值设为 1 来

表示自身能够执行的信息交换过程。算法区域 210 的长度是 16 比特，所以最大能够表示 16 种信息交换过程。最大数据长度 212 表示在发收 AKE 命令及与其对应的响应时、能够接收的最大数据长度为多少字节。

图 3C 表示 AKE 控制命令的格式。AKE 控制命令中的算法区域 201 在算法 ID 200 的值为 0 时，表示执行中的信息交换过程。算法区域 201 的各比特在 AKE 控制命令及与 AKE 控制命令对应的响应中，必然只有 1 个比特为 1，而其他比特为 0，该值 1 的 1 个比特表示当前执行中的信息交换过程。标号(label)202 用于明确多个 AKE 控制命令间的对应。例如，假设 1 个装置对另一个装置发送 AKE 控制命令，而且假设在某个信息交换过程中有下述规定，即，接收到该 AKE 控制命令的装置返送与接收到的 AKE 控制命令呼应的另一个 AKE 控制命令。在此情况下，为了明确两 AKE 控制命令间的呼应关系，插入到返送的 AKE 控制命令中的标号 202、与插入到最初接收到的 AKE 控制命令中的标号 202 使用同一值。步骤号码 203 是按照信息交换过程中发收的过程、对各个 AKE 控制命令从 1 开始依次赋予的序号。

子功能 299 取表 1 所示的值，通过该值来确定该 AKE 命令具有的意义。

表 1

| 子功能 | 值 |
|---|---|
| 作出响应(メイクレスポンス) | $00_{16}$ |
| 向我确认(ベリファイミー) | $01_{16}$ |
| 创建密钥信息(クリエイトキーインフォ) | $10_{16}$ |
| 重建密钥(リコンストラクトキー) | $11_{16}$ |
| 交换(エクスチェンジ) | $20_{16}$ |

在子功能 299 的内容是作出响应的情况下，该 AKE 控制命令表示对接收命令的装置的认证的质问(challenge)。此时，在数据 207 中，包含认证质问数据，它是用于认证对方装置的随机数。接收到该命令的装置返送子功能 299 内容为向我确认的 AKE 控制命令。在该返送时，数据 207 中容纳的数据是表示对刚才接收到的数据 207 中的认证质问数据进行预定运算所得结果的认证响应数据。该运算所用的密钥信息是预先只对被认定是正规的设备赋予的密钥，所以如果检查返送来的认证响应数据，就能够认证进行运算的设备是否是被认定为正规的设备。

在子功能 299 的内容是创建密钥信息的情况下，该 AKE 控制命令表示

向接收该命令的装置请求加密密钥 109。接收到该 AKE 控制命令的装置返送子功能 299 内容为重建密钥的 AKE 控制命令。此时，在返送的数据 207 中包含加密过的加密密钥 109。

在子功能 299 的内容是交换的情况下，该 AKE 控制命令表示发送命令的设备、和接收命令的设备之间密钥信息的交换。该密钥信息被容纳在数据 207 中传送，用于设备间的间接认证、和设备公共密钥的制作。

表 1 所举的值以外的子功能值是为将来的扩展而保留的。信道号码 204 表示在发送装置 110 和接收装置 128 之间进行的同步通信的信道号码。该信道号码 204 只在子功能 299 的内容为创建密钥信息或重建密钥时有效，在此以外的情况下，该值为 16 进制表记 FF。块号码 205 及总块号码 206 用于要以 AKE 控制命令发收的数据用 1 个 AKE 命令传输不完的情况。即，在此情况下，该数据被分割为几个块，分多次传送。总块号码 206 表示分割该数据所得的块数，而块号码 205 表示数据 207 是第几块的数据。数据长度 209 用字节数表示包含在数据 207 中的有效数据长度。数据 207 是通过 AKE 控制命令发收的数据。接收到 AKE 控制命令的装置返回对该 AKE 控制命令的应答。此时的应答格式及值、与接收到的 AKE 控制命令的格式及值相同，唯一不同的一点是，在应答中不包含数据 207。

图 4 用时间序列示意性地示出从发送装置 110 向接收装置 128 发送加密密钥 109、126 期间、两装置间发收的 AV/C 命令的具体例。首先，简单地说明图 4 所示的 AV/C 命令的发收开始之前两装置的操作。

首先，作为初始状态，设想从发送装置 110 发送未加密的 TSP 的状况。从信号源 100 输出的 TSP 被输入到加密部件 101。加密部件 101 由于输出命令 105 的内容是通常输出，所以对 TSP 不加密，原封不动地输出到源分组化部件 102，同时作为加密信息 910 而输出值 0。源分组化部件 102 向接收到的 TSP 附加 4 字节的源分组首标，输出到 CIP 块化部件 103。CIP 块化部件 103 向此附加 8 字节的 CIP 首标 954，作为同步净荷 952 输出到同步分组化部件 107。此时，在 CIP 首标 954 中包含的加密信息 910 中，原封不动地容纳从加密部件 101 输入的值 0。同步分组化部件 107 向接收到的同步净荷 952 附加同步分组首标 900、首标 CRC 901 及数据 CRC 903，制作同步分组。该同步分组通过 1394 分组输入输出部件 108 输出到 1394 总线 111 上。此时，由于该同步分组是符合 AV 协议的同步分组，所以包含在同步分组首标 900

中的标记907的值为1。

在从信号源100输出的TSP变化时，即，从未用著作权保护的图像语音信息、向用著作权保护的图像语音信息切换时，检测出该变化的密钥生成部件106将输出命令105从通常输出变化为空输出，同时将用于对TSP进行加密的加密密钥109传递给加密部件101。

在输出命令105的内容是空输出时，加密部件101每当从信号源100接收到TSP时就向源分组化部件102输出空信号，同时作为加密信息910而输出值1。从加密部件101接收到空信号的源分组化部件102不附加源分组首标，而将接收到的空信号原封不动地传达到CIP块化部件103。CIP块化部件103一接收到空信号，就只将CIP首标954输出到同步分组化部件107。此时，CIP首标954中的加密信息910原封不动地使用加密部件101输出的值1。同步分组化部件107将从CIP块化部件103接收到的CIP首标954作为同步净荷952来制作同步分组，输出到1394分组输入输出部件108。此时，该同步分组符合AV协议，所以标记907的值为1。1394分组输入输出部件108将接收到的同步分组输出到1394总线111上。该同步分组被连续输出，在1394总线111上持续地流动同步净荷952中只包含CIP首标954的同步分组。在接收到该同步分组的接收装置128中，1394分组输入输出部件127检查标记907，在检测出是符合AV协议的同步分组之后，将该同步分组输出到净荷提取部件123。净荷提取部件123从接收到的同步分组中提取同步净荷952，输出到实数据提取部件122。实数据提取部件122将CIP首标954中包含的加密信息910和源ID 906输出到密钥生成部件125。密钥生成部件125检查加密信息910，在检测出值为1之后，由源ID 906知道输出该同步分组的是输出装置110。此后，移至密钥生成部件125使用AV/C命令来请求加密密钥109、126的过程、即图4所示的过程。

在图4中，首先AKE状态命令300被从接收装置128发送到发送装置110。由此，接收装置128询问发送装置110能够执行的信息交换过程。响应此，发送装置110将AKE响应301返送到接收装置128。在该AKE响应301中，发送装置110能够执行的信息交换过程被比特指定到算法区域201内，由此，接收装置128能够知道发送装置110能够执行哪种信息交换过程。作为具体例，在发送装置110能够执行的信息交换过程是第2个和第6个这2个的情况下，AKE响应301内的算法区域201为2进制表记

0000000000100010。

接收到 AKE 响应 301 的接收装置 128 从发送装置 110 能够执行、而且接收装置 128 自身也能够执行的信息交换过程中，选择最佳的 1 个过程，以后根据该过程来发收 AV/C 命令。现在假设在接收装置 128 端、能够执行的信息交换过程是第 2 个和第 8 个的情况下，发送装置 110 及接收装置 128 双方能够执行的信息交换过程只有第 2 个，以后使用第 2 个过程来进行认证及信息的交换。在该过程中包含的 AKE 控制命令中，算法 ID 的值为 0，算法区域 201 的值为 16 进制表记 0000000000000010。在信息交换过程指定的过程中，不仅规定了各种 AKE 控制命令的发收的顺序，也规定了各 AKE 控制命令发送的数据 207 的格式和处理方法。

根据第 2 个信息交换过程，密钥生成部件 125 将作出响应命令 302 发送到发送装置 110。在该作出响应命令 302 中的数据 207 中，包含密钥生成部件 125 产生的、被加密的 2 个随机数 RRa 和 RRb，同时在算法区域 201 中包含表示第 2 个过程的识别信息。在该加密时使用的密钥是预先提供给被认为是正规的发送装置和接收装置的公共秘密密钥。接收到作出响应命令 302 的密钥生成部件 106 检查接收到的作出响应命令 302 的算法区域 201，知道以后使用第 2 个过程进行认证及信息的交换。密钥生成部件 106 能够执行第 2 个过程，所以知道在根据第 2 个过程发送来的作出响应命令 302 的数据 207 中包含有用该秘密密钥加密过的 2 个随机数。因此，密钥生成部件 106 使用该秘密密钥从数据 207 中取出 RRa 及 RRb 这 2 个随机数之后，返回表示能够制作响应的应答 303。此后，密钥生成部件 106 将取出的随机数中的 1 个、即 RRa 容纳到数据 207 中，将向我确认命令 304 发送到接收装置 128。这是刚才的作出响应命令 302 所请求的响应。包含该向我确认命令 304，此后，在发送装置 110 和接收装置 128 之间发收的各 AKE 命令的算法区域 201 中，都包含表示第 2 个过程的识别信息。

接收到向我确认命令 304 的密钥生成部件 125 在确认数据 207 的内容 RRa 与自己刚才产生的随机数 RRa 一致之后，对应于向我确认命令 304，返回表示确认为正常的应答 305。由此，密钥生成部件 125 认证发送装置 110 为被认为是正规的发送装置。

接着，发送装置 110 通过与上述作出响应 302 以后相同的过程，使用作出响应命令 306、及向我确认命令 308，确认接收装置 128 是被认为是正规

的接收装置。然而，此时使用的随机数是 RTa 及 RTb，用向我确认命令 308 返送的随机数是 RTb。

此刻，发送装置 110 及接收装置 128 双方都知道随机数 RRb 和随机数 RTb，此外，相互确认为是被认为是正规的装置。密钥生成部件 106 和密钥生成部件 125 分别通过第 2 个过程规定的公共运算方法，由 RRb 和 RTb 来生成临时密钥(未图示)。该临时密钥是只有发送装置 110 及接收装置 128 这两装置共有的公共密钥。

接着，密钥生成部件 125 将创建密钥信息命令 310 发送到发送装置 110。此时，在创建密钥信息命令 310 的信道号码 204 中，容纳有当前接收装置 128 正在接收的同步分组的信道号码。接收到该创建密钥信息命令 310 的密钥生成部件 106 将 TSP 加密所用的加密密钥 109 用上述临时密钥加密之后，返送表示创建密钥信息命令 310 正常结束的应答 311。接着，密钥生成部件 106 将数据 207 中容纳有用临时密钥加密该加密密钥 109 所得的结果的重建密钥命令 312 发送到接收装置 128。密钥生成部件 125 使用临时密钥，对接收到的重建密钥命令 312 的数据 207 进行解密，结果，得到加密密钥 126 之后，返回表示正常结束重建密钥命令 312 的应答 313。加密密钥 109 和加密密钥 126 使用同一临时密钥进行加密和解密，所以是同一密钥。该加密密钥 126 从密钥生成部件 125 输出到解密部件 121。用以上过程结束解密信息的赋予。

发送重建密钥命令 312 的密钥生成部件 106 向加密部件 101 输出表示加密输出的输出命令 105。接收到此的加密部件 101 用加密密钥 109 对从信号源 100 接收到的 TSP 进行加密，开始向源分组化部件 102 的输出。由此，在 1394 总线 111 上，将同步净荷 952 中包含用加密密钥 109 加密过的 TSP 的同步分组从发送装置 110 发送。接收装置 128 接收到的该同步分组如前所述，在解密部件 121 中使用加密密钥 126 被解密，输出到图像语音化部件 120。

在上述一系列 AKE 控制命令中，作出响应命令 302 和向我确认命令 304、作出响应命令 306 和向我确认命令 308、作出响应命令 310 和向我确认命令 312 分别具有相同的标号 202。此外，作出响应命令 302、向我确认命令 304、作出响应命令 306、向我确认命令 308、作出响应命令 310、向我确认命令 312 分别具有 1、2、3、4、5、6 的值作为步骤号码 203。

在发送装置 110 输出的同步分组中包含的实数据部 105 从加密过的实数据 105 变化到未加密的实数据 105 的情况下，解密部件 121 检测出加密信息

910 的变化后停止解密，将从实数据提取部件 122 接收到的输出原封不动地传递给图像语音化部件 120。

此外，在上述图 4 所示的过程开始之后，在 1394 总线 111 上发生总线复位的情况下，从开始重新进行作出响应命令 302 以后的过程。

如上所述，根据本实施例，通过将表示同步分组内实数据加密状况的加密信息和实数据一起从发送装置发送，接收到同步分组的接收装置检查同步分组内包含的加密信息，如果检测出实数据被加密，则向发送装置请求用于对实数据进行解密的加密密钥，接收到请求的发送装置对该接收装置赋予加密密钥，所以能够实现发送装置向接收装置赋予用于解密的加密密钥时的过程极其简单的数据传送方法。

此外，如上所述，根据本实施例，在用同步通信传送的同步分组中，包含表示实数据加密状况的加密信息和实数据，通过只对实数据进行加密进行数据传送，能够实现一种数据传送方法，使得保持与以往数据传送方法的兼容性，而且以往的接收装置即使接收加密过的实数据，也不可能误操作。

此外，如上所述，根据本实施例，即使在接收装置连续接收发送装置发送的同步数据期间，同步数据的加密开始，CIP 首标也不被加密而是原封不动地传送，所以可以实现一种数据传送方法，使得进行接收的接收装置不可能误操作。

在本实施例中，由加密密钥进行的加密一旦开始，所有的传送单位中包含的实数据都被加密而发送，但是没有必要对所有的传送单位进行加密。例如，即使加密过的传送单位和未加密的传送单位被交替发送，由于 CIP 首标中包含加密信息，所以在接收装置中也能够正常进行解密，能够得到同样的效果。再者，在此情况下，接收装置向发送装置指定进行加密的传送单位的比例，得到的效果当然也不变。然而，MPEG 的源分组的大小是 192 字节，但是在进行 MPEG 的高数据率传送(12Mbps 以上)时，多个源分组被容纳到 1 个同步净荷中。此时，在同一同步净荷中，当然不能既有加密过的源分组、又有未加密的源分组。

在本实施例中，由加密密钥进行的加密对所有实数据进行，但是没有必要对所有部分进行加密。例如，只对实数据部的前半部分进行加密，或者将实数据部的 4 等分中最初和第 3 个这两处进行加密来发送也能得到同样的效果。在此情况下，如果将进行加密的部分和比例的信息插入到 CIP 首标中来

发送，则在接收装置端能够进行适当的解密。再者，在 CIP 首标中，只插入表示实数据是否被加密的加密信息，看到 CIP 首标而检测出被加密的接收装置通过同步通信向发送装置询问实数据部的哪个部分被如何加密这一信息，也能够得到同样的效果。在此情况下，接收装置向发送装置使用异步通信来指定进行加密的部分和比例，当然也能够得到同样的效果。此外，如果只对实数据部中数据重要性高的部分进行加密，则加密及解密的负荷降低，而且当然也能够得到充分的加密效果。

在本实施例中，在发送装置和接收装置之间的相互认证结束之前，只传送不包含实数据的 CIP 首标的同步分组，但是不只输出 CIP 首标的同步分组，而是输出包含从一开始就加密过的实数据的同步分组，当然也能够得到同样的效果。

在本实施例中，在发送装置和接收装置之间发收的 AKE 控制命令的传送过程是通过相互协商来决定的，但是在接收装置能够执行的过程只限于一个的情况下，不进行该协商过程，而是用接收装置能够执行的唯一过程来开始命令的传送，当然也能够得到同样的效果。在此情况下，最好预先确定所有被认证为是正规的设备最低限能够执行的基本过程。

在本实施例中，在发送装置和接收装置之间进行直接认证，传送由秘密密钥进行的解密信息，但是认证及解密信息的传达手段不限于此。例如，也可以使用公开密钥相互进行间接认证及临时密钥的制作，使用临时密钥进行解密信息的传输。下面，简单说明其过程。

发送装置及接收装置通过相互协商而定的过程，将相互间接认证所需的密钥信息容纳到 AKE 控制命令的数据 207 中相互发送。此时，子功能 299 表示交换。由此，如果发送装置和接收装置是相互认证是正规的设备，则共有相同的临时密钥，所以其后能够用与本实施例同样的过程，使用创建密钥信息命令及重建密钥命令来传输解密信息。

在本实施例中，在发送装置和接收装置之间发收的 AKE 控制命令的传送过程是通过相互协商来决定的，但是在发送装置能够执行的过程的种类预先知道的情况下，不进行该协商过程，接收装置就用发送装置能够执行的过程开始命令的传送，当然也能够得到同样的效果。

在本实施例中，在发送装置和接收装置之间发收的 AKE 控制命令的传送过程是通过相互协商来决定的，但是决定传送过程的手段不限于此。即，

在多个传送过程各具有预定的优先级的情况下，接收装置使用自身能够执行的过程中优先级最高的过程开始传送，在发送装置不能执行该过程的情况下，按照优先级依次选择下一个过程开始传送，如果知道发送装置和接收装置双方都能够执行的过程，则使用该过程来传送 AKE 控制命令，当然也能够得到同样的效果。

在本实施例中，发送装置对实数据部的解密所用的解密信息进行加密而传送到接收装置，但是接收装置取得解密信息的手段不限于此。即，也可以不传送发送装置加密过的解密信息，而是发送装置向接收装置传送接收装置足以取得解密信息的信息，接收装置由该信息间接取得解密信息。具体地说，从发送装置向接收装置只传送散列(hash)函数的种源，在接收装置端根据接收到的种源使用散列函数来取得解密信息，当然也能够得到同样的效果。

在本实施例中，示出 AKE 命令的格式的一例，但是 AKE 命令的格式不限于此。即，本实施例所示的 AKE 命令的格式不过是用于实现本实施例的一例，使用与此不同的格式的命令当然也能够得到同样的效果。

产业上的可利用性

如上所述，在本发明的数据传送方法中，通过将表示同步数据内实数据部加密状况的加密识别信息和实数据部一起发送进行数据传送，接收到同步数据的接收装置检查同步数据内包含的加密识别信息，如果检测出实数据部被加密，则向发送装置请求用于对实数据部进行解密的解密信息，接收到该请求的发送装置向接收装置赋予解密信息，所以其有益效果是，能够实现发送装置向接收装置赋予用于解密的密钥信息时的过程极其简单的数据传送方法。

此外，如上所述，在本发明的数据传送方法中，在用同步通信传送的同步数据中包含表示实数据部加密状况的加密识别信息和实数据部，通过只对实数据部加密进行数据传送，其有益效果是能够实现一种数据传送方法，使得保持与以往数据传送方法的兼容性，而且即使以往的接收装置接收加密过的同步数据，也不可能误操作。

此外，如上所述，在本发明的数据传送方法中，在用同步通信传送的同步数据中包含表示实数据部加密状况的加密识别信息和实数据部，通过只对实数据部加密进行数据传送，其有益效果是能够实现一种数据传送方法，即

使在接收装置连续接收发送装置发送的同步数据期间，同步数据的加密开始，由于 CIP 首标不被加密而是原封不动地传送，所以进行接收的接收装置不可能误操作。

此外，如上所述，在本发明的数据传送方法中，通过发送装置和接收装置之间的协商来选择在发送装置和接收装置之间发收的认证信息及解密信息的授受过程，从而能够实现将来扩展性优越的认证及解密信息的授受过程。即，在将来新认证方法和解密信息能够利用时，即使混用能够使用新过程的设备和只能使用旧过程的设备，如果新设备能够使用旧过程，则通过两设备间的协商能够选择最佳的过程。即，采用本发明的数据传送方法的有益效果是，即使在混用新设备和旧设备的环境下，也能够始终选择最佳的过程来执行。

此外，如上所述，在本发明的数据传送方法中，能够变化加密过的实数据和未加密的实数据的比例，所以即使接收装置不具有能够对加密过的实数据进行解密的高速处理的专用硬件，也能够通过软件进行解密。即，其有益效果是，在个人计算机这样不具有解密用的硬件的设备作为接收装置的情况下，也能够通过降低加密实数据的比例而减少解密处理，从而由处理速度慢的软件进行解密。

此外，如上所述，在本发明的数据传送方法中，在发送装置和接收装置相互认证是正规的设备之前这一期间内，输出不包含实数据的同步分组，所以其有益的效果是，不会浪费总线有限的传送频带，此外，未被认证是正规的设备接收到实数据的可能性变得非常小。

# 说 明 书 附 图

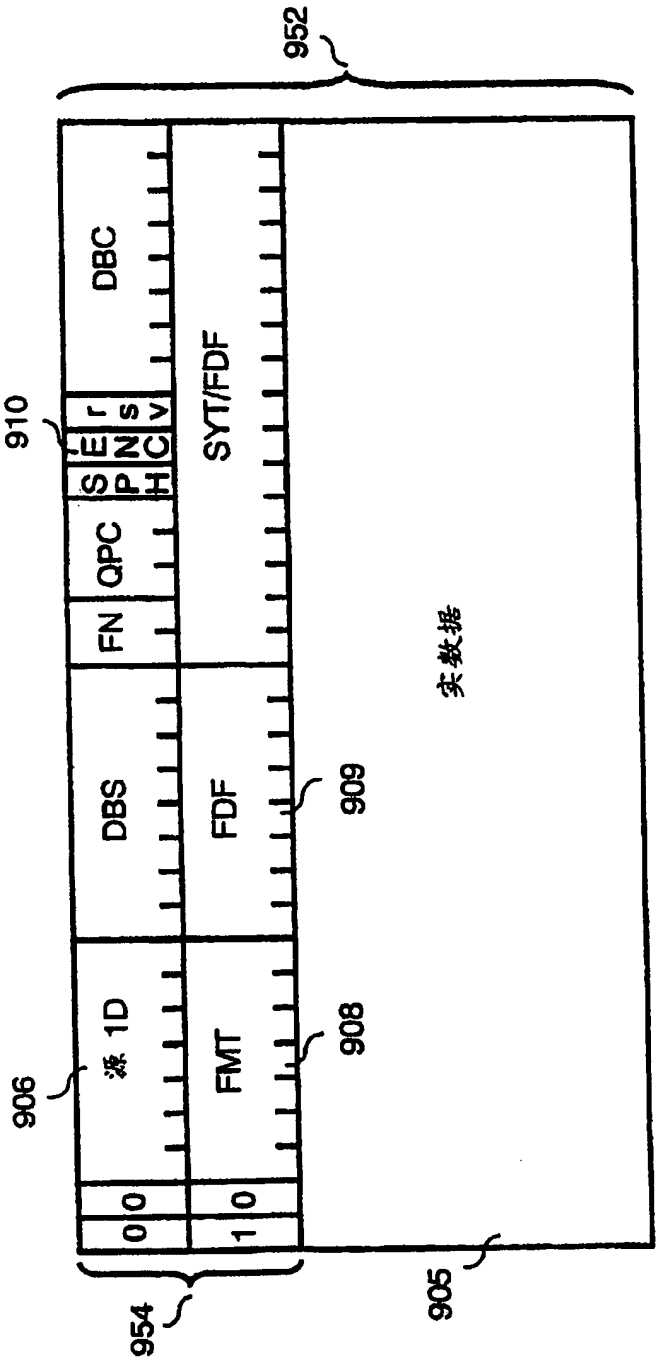

952
910
906
908
909
905
954
0
0
1
0
源 1D
FMT
DBS
FDF
FN
QPC
S
P
H
E
N
C
r
s
v
DBC
SYT/FDF
实数据

图 1

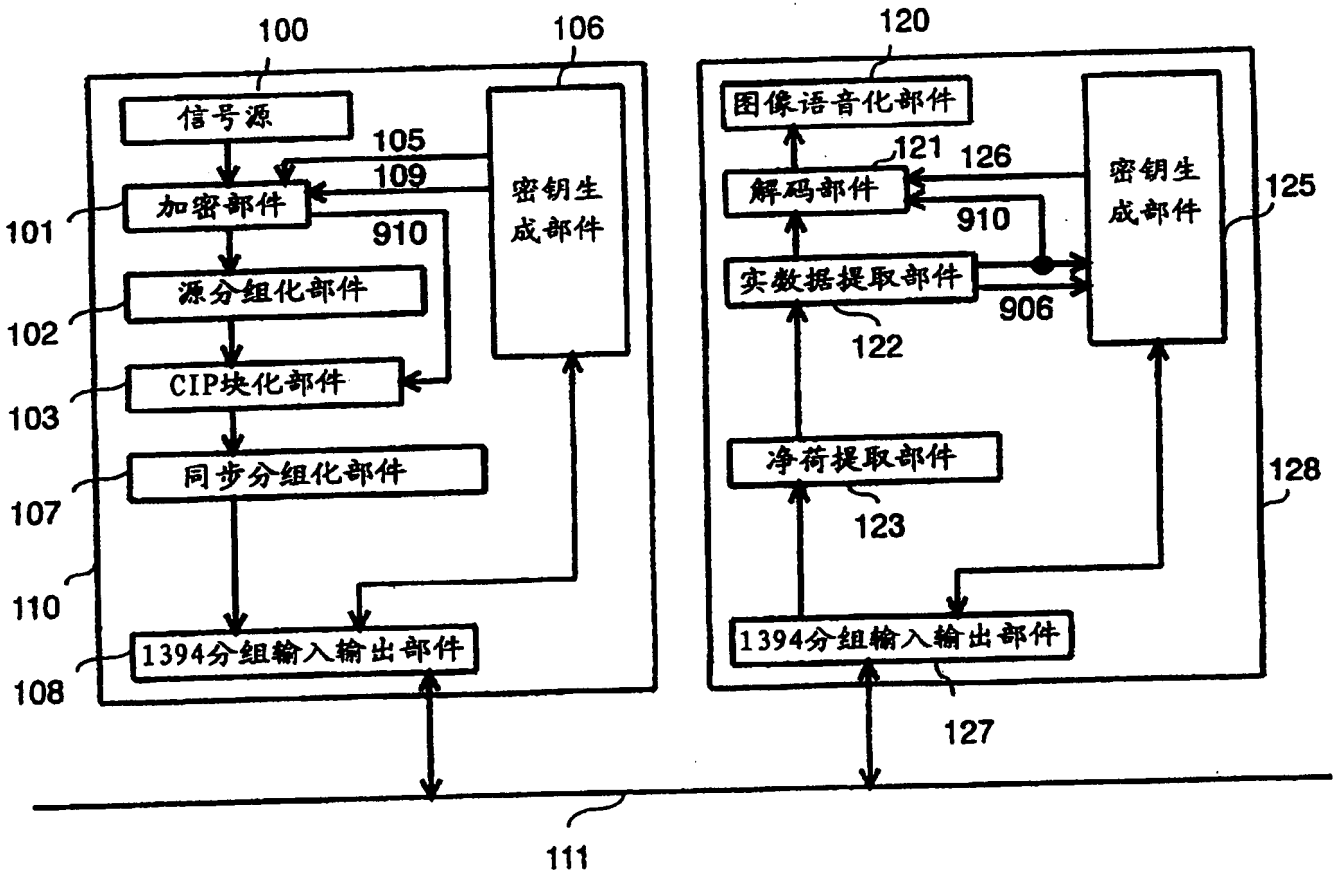

100
106
120
信号源
105
109
密钥生成部件
101
加密部件
910
源分组化部件
102
CIP块化部件
103
同步分组化部件
107
110
1394分组输入输出部件
108
图像语音化部件
121
126
解码部件
910
125
实数据提取部件
906
122
净荷提取部件
123
128
1394分组输入输出部件
127
111

图 2

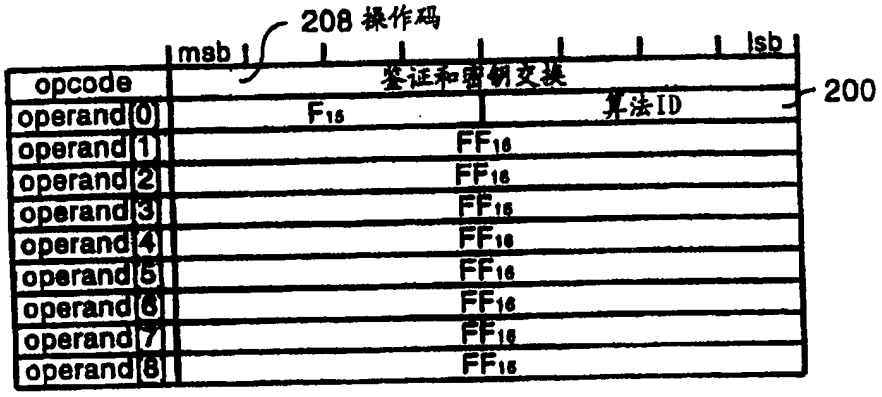

208 操作码
msb
lsb
opcode
鉴证和密钥交换
200
operand [0]
F15
算法ID
operand [1]
FF16
operand [2]
FF16
operand [3]
FF16
operand [4]
FF16
operand [5]
FF16
operand [6]
FF16
operand [7]
FF16
operand [8]
FF16

图 3A

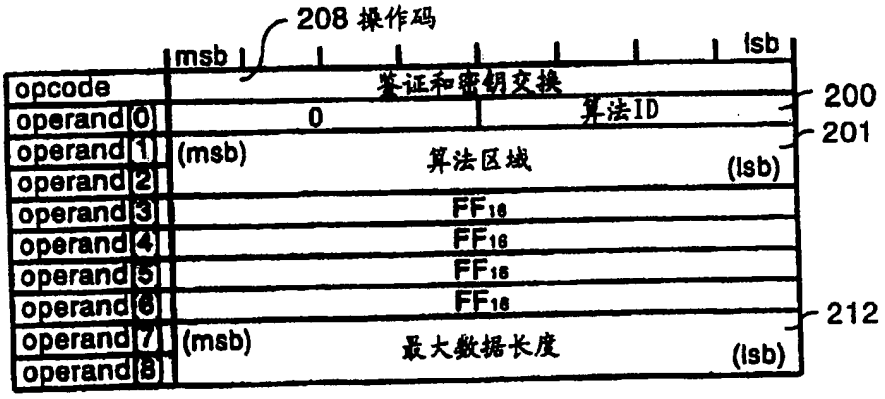

208 操作码
msb
lsb
opcode
鉴证和密钥交换
200
operand [0]
0
算法ID
201
operand [1]
(msb)
算法区域
(lsb)
operand [2]
operand [3]
FF16
operand [4]
FF16
operand [5]
FF16
operand [6]
FF16
212
operand [7]
(msb)
最大数据长度
(lsb)
operand [8]

图 3B

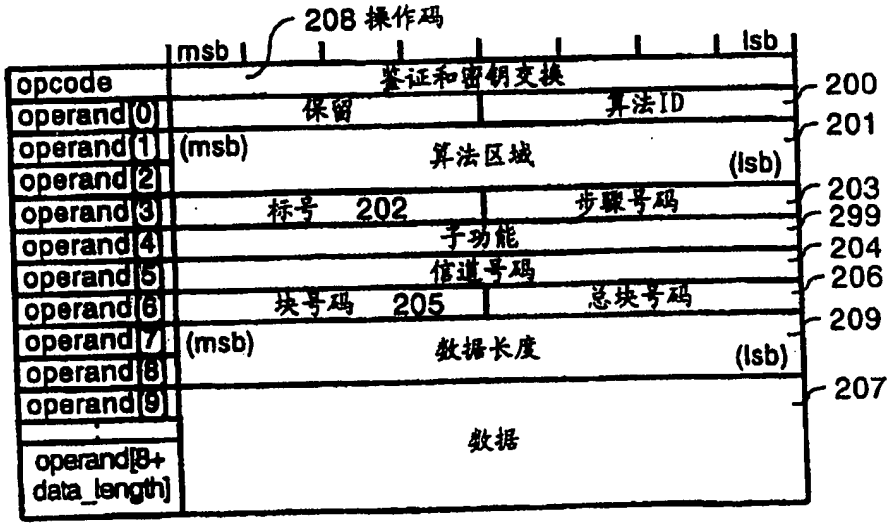

208 操作码
msb
lsb
opcode
鉴证和密钥交换
200
operand [0]
保留
算法ID
201
operand [1]
(msb)
算法区域
(lsb)
operand [2]
operand [3]
标号 202
步骤号码
203
299
operand [4]
子功能
204
operand [5]
信道号码
206
operand [6]
块号码 205
总块号码
209
operand [7]
(msb)
数据长度
(lsb)
operand [8]
207
operand [9]
数据
operand[8+ data_length]

图 3C

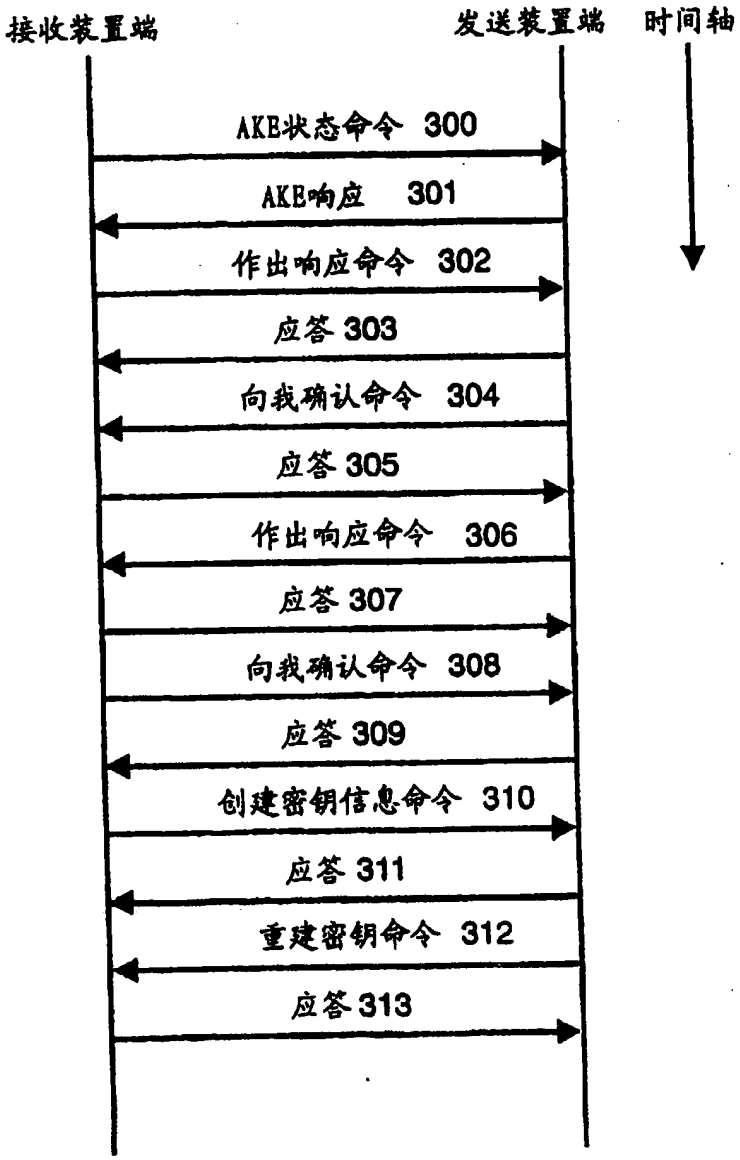

接收装置端
发送装置端
时间轴
AKE状态命令 300
AKE响应 301
作出响应命令 302
应答 303
向我确认命令 304
应答 305
作出响应命令 306
应答 307
向我确认命令 308
应答 309
创建密钥信息命令 310
应答 311
重建密钥命令 312
应答 313

图 4

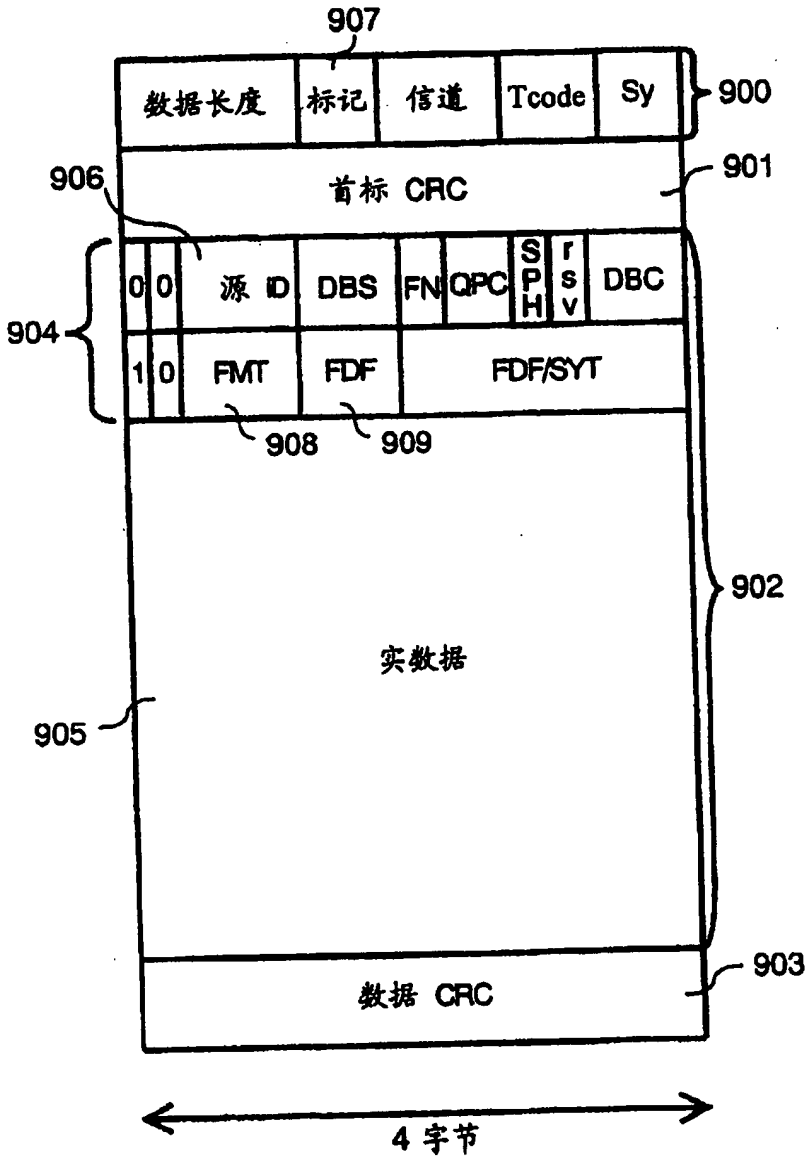

907
数据长度
标记
信道
Tcode
Sy
900
首标 CRC
901
906
0
0
源 ID
DBS
FN
QPC
SPH
rsv
DBC
904
1
0
FMT
FDF
FDF/SYT
908
909
902
实数据
905
903
数据 CRC
4 字节

图 5

附图参考符号一览表

100 信号源

101 加密部件

102 源分组化部件

103 CIP 块化部件

107 同步分组化部件

108、127 1394 分组输入输出部件

105 输出命令

109、126 加密密钥

110 发送装置

128 接收装置

111 IEEE1394 总线

106、125 密钥生成部件

120 图像语音化部件

121 复合化部件

122 实数据提取部件

123 净荷提取部件

200 算法 ID

201 算法区域

202 标号

203 步骤号码

204 信道号码

205 块号码

206 总块数

207 数据

208 操作码

209 数据长度

212 最大数据长度

299 子功能

300 AKE 状态命令

301 AKE 响应

302、306　　作出响应命令

303、305、307、309、311、313　应答

304、308　　向我确认命令

310　创建密钥信息命令

312　重建密钥命令

900　同步分组首标

901　首标 CRC

902、952　　同步净荷

903　数据 CRC

904、954　　CIP 首标

905　实数据

906　源 ID

907　标记

908　FMT

909　FDF

910　加密信息(ENC)

952　同步净荷